UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

NITAYA MCGEE, individually and on behalf of all others similarly situated, Plaintiff, v. JUST A BABY, INC., Defendant.	Case No. CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Dated: March 10, 2025

BURSOR & FISHER, P.A.
Yitzchak Kopel
Max S. Roberts
Victoria X. Zhou
1330 Avenue of the America, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: ykopel@bursor.com
mroberts@bursor.com
vzhou@bursor.com

Attorneys for Plaintiffs

Plaintiff Nitaya McGee files this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Just A Baby, Inc. ("Defendant"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all California residents who have accessed and used the mobile application owned and operated by Just A Baby, Inc., on Apple devices (the "App").

2. On the App, users can, *inter alia*, connect with other App users to find a surrogate, partner, co-parent, sperm, or egg donor. Defendant explains that "Just a Baby is the fastest growing community connecting you with thousands of people worldwide open to discussing surrogacy, donation and co-parenting."[1]

3. Defendant's App is used by "sperm donor[s], egg donor[s], embryo donor[s and] surrogate[s,]" "someone willing to co-parent[,]" and for those who want to "help others start a family[.]"[2] When using the App, App users provide Defendant with sensitive information, including "medical information" under Cal. Civil Code § 56.05.

4. Unbeknownst to Plaintiff and Class Members, however, Defendant aids, employs, agrees with, or otherwise enables third party Twilio, Inc. d/b/a Twilio Segment ("Segment" or "Third Party") to eavesdrop on communications sent and received by Plaintiff and Class Members, including communications containing protected medical information, using Segment's wiretap, as set out *infra*.

---

[1] JUST A BABY: BECOME A PARENT, APP STORE, https://apps.apple.com/us/app/just-a-baby-become-a-parent/id1147759844.

[2] *Id.*

5. Plaintiff brings this action for legal and equitable remedies resulting from these illegal actions.

PARTIES

6. Plaintiff Nitaya McGee is, and has been at all relevant times, a resident and citizen of Riverside, California. In or around January 2025, Plaintiff McGee created a Just A Baby account and signed into her account on the App on her Apple device. Numerous times, including on or around January 26, 2025, Plaintiff McGee accessed Defendant's App. Plaintiff McGee was in California when she accessed the App. Upon accessing the App, as alleged in greater detail below, Plaintiff McGee communicated with the App—and searched for, connected, and communicated with individuals on the App—seeking to conceive a child through alternative conception methods. Each of these communications was intercepted in transit by Third Party Twilio, Inc. d/b/a Twilio Segment ("Segment"), as enabled by Defendant. Neither Defendant nor Segment procured Plaintiff Mcgee's prior consent to this interception.

7. Defendant Just A Baby, Inc. is a Delaware corporation with its principal place of business at 31 Driggs Ave, GreenPoint, Brooklyn NY.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action where there are more than 100 members and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one member of the putative Class is a citizen of a state different from Defendant.

9. The Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant maintains its principal place of business in this District.

FACTUAL ALLEGATIONS

I. THE CALIFORNIA INVASION OF PRIVACY ACT

11. The California Legislature enacted the Invasion of Privacy Act to protect certain privacy rights of California citizens. The legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

12. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

13. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas v. Clark, 38 Cal. 3d 355, 360-61 (1985) (emphasis added; internal citations omitted).

14. As part of CIPA, the California Legislature enacted § 631(a), which prohibits any person or entity from [i] "intentionally tap[ping], or mak[ing] any unauthorized connection … with any telegraph or telephone wire," [ii] "willfully and without the consent of all parties to the communication … read[ing], or attempt[ing] to read, or to learn the contents or meaning of any …

communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California],” or [iii] “us[ing], or attempt[ing] to use … any information so obtained.”

15. CIPA § 631(a) also penalizes [iv] those who “aid[], agree[] with, employ[], or conspire[] with any person” who conducts the aforementioned wiretapping, or those who “permit” the wiretapping.

16. As part of the Invasion of Privacy Act, the California Legislature additionally introduced Penal Code § 632(a), which prohibits any person or entity from “intentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication.”

17. A “confidential communication” for the purposes of CIPA § 632 is “any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto.” Cal. Penal Code § 632(c).

18. Individuals may bring an action against the violator of CIPA §§ 631 and 632 for $5,000 per violation. Cal. Penal Code § 637.2(a)(1). Plaintiff does so here against Defendant.

II. THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT

19. Pursuant to the CMIA, a “provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c).” Cal Civ. Code § 56.10(a). “An authorization for the release of medical information . . . shall be valid if it:

(a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.

(b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.

(c) Is signed and dated . . .

(d) States the specific uses and limitations on the types of medical information to be disclosed.

(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.

(f) States the name or functions of the persons or entities authorized to receive the medical information.

(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization."

Cal. Civ. Code § 56.11.

20. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that records and discloses online patients' PII and PHI. Cal. Civ. Code § 56.36(c). Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

21. "In addition to any other remedies available at law, an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, it is not necessary that the plaintiff suffered or was threatened with actual damages. [¶] (2) The amount of

actual damages, if any, sustained by the patient." Cal. Civ. Code § 56.36(b).

III. TESTING REVEALS THAT DEFENDANT ILLEGALLY SHARES USERS' COMMUNICATIONS AND PII WITH A THIRD PARTY THROUGH THE APP

22. Third party Twilio, Inc., d/b/a Twilio Segment ("Segment"), wiretaps the App with its tracking technologies, which Defendant purposefully installed on the App.

23. In the Winter of 2025, Plaintiffs' counsel commissioned a private research company to review and conduct a dynamic analysis on the App. A "dynamic analysis" records the transmissions that occur from a user's device.

24. The private researchers tested what information (if any) Defendant discloses when an App user enters and interacts with the App. The analysis revealed that Defendant discloses to a third party its App users' (i) private communications, including communications relating to fertility information, relationship status, and users' written profile descriptions; and (ii) App users' personally identifiable information.

25. The analysis first established that Defendant incorporates an "application programming interface" ("API") into the Just a Baby App, either directly or contained inside a software development kit ("SDK").

26. APIs "enable[] companies to open up their applications' data and functionality to external third-party developers, business partners, and internal departments within their companies."[3]

27. Defendant integrates at least one company's API into the App: the Segment API. As alleged in greater detail below, Defendant discloses to Segment—via the Segment API—App users' (i) communications regarding protected medical information (including relationship status,

[3] APPLICATION PROGRAMMING INTERFACE (API), IBM, https://www.ibm.com/cloud/learn/api (last accessed Mar. 27, 2024).

fertility information, and written profile description) and (ii) personally identifiable information (including name, phone number, and birthdate), in addition to other information.

Summary of Third-Party Exfiltration

THIRD PARTY	WIRETAPPING INFO	PERSONAL INFO	OTHER INFO
Segment.io	User Intake Inputs*	Name, Phone Number, Birthdate	UserID, IP Address

IV. OVERVIEW OF THE SEGMENT API

28. Segment brands itself as an "[t]he leading customer data platform, powered by AI."[4] Segment develops, owns, and operates the SDK and API of the same name.

29. Segment boasts that "[t]he Segment Mobile SDKs are the best way to simplify tracking in your iOS … apps."[5]

30. Once integrated into a mobile application, the Segment API allows an app developer to, among other features, "[c]ollect, unify, and activate all your first-party data in a single platform to power personalized customer experiences[,]" and "[t]rack how users interact with your product, identify new or existing customers, and locate what page they were on or what device they were using when they performed an action."[6]

31. Segment goes on to explain that app developers may "[c]ollect user events from any platform with our analytics API." Indeed, Apple is a "[m]obile" "source[listed] on the Segment platform[.]"[7]

---

[4] TWILIO SEGMENT, https://segment.com/. Twilio has acquired Segment. https://help.twilio.com/articles/360056928254-What-is-Segment-and-why-did-Twilio-acquire-it.

[5] SEGMENT, HOW SEGMENT WORKS, https://segment.com/docs/getting-started/01-what-is-segment/.

[6] TWILIO SEGMENT, SEGMENT CONNECTIONS, https://segment.com/product/connections/?ref=nav.

[7] SEGMENT, SOURCES CATALOG, https://segment.com/docs/connections/sources/catalog/.

32. Segment analyzes user behavior through"[c]ore tracking methods" [8] that (i) "[t]rack," which "lets you record the actions your users perform[,]"[9] (ii) "[i]dentify[,]" which "lets you tie a user to their actions and record traits about them" and "includes a unique user ID and any optional traits you know about them like their email, name, or address[,]" (iii) "[s]creen[,]"which "lets you record whenever a user sees a screen in your mobile app, along with optional extra information about the page being viewed[,]"; "[g]roup[,]" which "lets you associate an individual user with a group[,]"and "[a]lias[,]" which "is used to merge two user identities, effectively connecting two sets of user data as one."[10]

33. In turn, clients like Defendant "can send data from iOS … applications to any analytics or marketing tool without having to learn, test, or implement a new API every time."[11]

34. Segment goes on to explain that this data may be captured in real-time: "When you capture interaction data in Segment, you can send it (often in real-time) to your marketing, product, and analytics tools, as well as to data warehouses."[12]

35. As part of Segment's suite of data capabilities, once a client has "collected your interaction data," that same client can "[u]se Engage, [a] marketing automation tool, to build marketing campaigns personalized to your audience."[13] This marketing tool allows clients to

---

[8] SEGMENT, ANALYTICS-SWIFT FOR IOS & APPLE, https://segment.com/docs/connections/sources/catalog/libraries/mobile/apple/.

[9] SEGMENT, ANALYTICS-SWIFT IMPLEMENTATION GUIDE, https://segment.com/docs/connections/sources/catalog/libraries/mobile/apple/implementation/.

[10] *Id.*

[11] SEGMENT, ANALYTICS-SWIFT FOR IOS & APPLE, https://segment.com/docs/connections/sources/catalog/libraries/mobile/apple/.

[12] SEGMENT, WHAT IS SEGMENT? https://segment.com/docs/getting-started/.

[13] SEGMENT, HOW SEGMENT WORKS, https://segment.com/docs/getting-started/01-what-is-segment/.

"[c]reate unified customer profiles" and target customers through "send[ing] an SMS, email, or WhatsApp campaign[.]"[14]

36. Segment also collects this data so its clients can better target advertisements. Specifically, Segment compiles and transmits information to other third parties for targeted advertising.[15] Segment labels these third parties "Segment Destinations," and include, for example, Google Ads.[16] In this role, Segment acts as a facilitator, compiling PII and private communications so developers can "personalize messages across channels, optimize ad spend, and improve targeting."[17]

37. As alleged in greater detail below, Defendants utilize each and every one of these features and sends App users' communications and PII to Segment through the Segment API to assist with Defendant's marketing, advertising, and analytics efforts.

V. DEFENDANT AIDS, AGREES WITH, EMPLOYS, OR OTHERWISE ENABLES THE THIRD PARTIES TO WIRETAP CALIFORNIANS' COMMUNICATIONS

38. App users' private communications are the product of App users affirmatively entering, and interacting with, information on the App (*i.e.*, the private communications are not procedurally or automatically generated). Indeed, the private communications stem from App users typing into data fields, conveying responses to questions and prompts, and actively making other selections. All of the foregoing is information created through the intent of App users:

---

[14] SEGMENT, ENGAGE INTRODUCTION, https://segment.com/docs/engage/.

[15] *See* SEGMENT, USING ENGAGE DATA, https://segment.com/docs/engage/using-engage-data/ ("Every time a piece of data (such as a track event or identify call) is received in Segment — for example, from your website *or your mobile app* — Segment then sends this piece of data to the Destination right away.") (emphasis added).

[16] SEGMENT, GOOGLE ADS (CLASSIC) DESTINATION, https://segment.com/docs/connections/destinations/catalog/google-ads-classic/.

[17] SEGMENT, USING ENGAGE DATA, https://segment.com/docs/engage/using-engage-data/.

information created by and in response to App users' communicative inputs; information created by and in response to App users' intended messages to the App, other App users, and/or Defendant; and information created by and in response to App users' having conveyed and expressed their respective desires that the App would supply them with certain, highly personalized, types of information and/or responses.

39. Segment, as enabled by Defendant, contemporaneously intercepts the following App communications.


```
outbound to api.segment.io:443 at time Wed 11 Dec 2024, 15:04:18.372188
(1733929458.3721879) uuid be0e1646-9579-4b18-8186-9cdb88e6b365
-------------------------------
POST /v1/b HTTP/1.1
user-agent: analytics-flutter/1.0.0
content-type: application/json; charset=utf-8
accept-encoding: gzip
content-length: 24772
host: api.segment.io
…
"batch": [{"_metadata": {
…
"event": "send_code",
"integrations": "",
"messageId": "3a91a472-5d4b-45ba-9e40-f655d2373cbf",
"properties": {
"ApInstanceId": "1494FB8F94B04CC28534857CDA4CF536",
"number": "9179924278",
"screen_name": "login_mobile"
},
"timestamp": "2024-12-11T10:04:02.741801",
"type": "track",
"userId": ""
…
"event": "ipAddress",
"integrations": "",
"messageId": "bda2cc6d-8787-4b9d-81e2-3c2b8db5a4f5",
"properties": {
"ApInstanceId": "1494FB8F94B04CC28534857CDA4CF536",
"ip": "76.240.242.167",
"screen_name": "InitStore"
},
"timestamp": "2024-12-11T10:04:18.172719",
"type": "track",
"userId": "YYS0LcqBKg"
}
```

40. As shown by the blue highlight in the above excerpt of the App's transmissions, Segment intercepts the phone number of the App user (here, "9179924278"). As shown by the red highlight, Segment intercepts the IP address of the App user (here, "76.240.242.167").


```
outbound to api.segment.io:443 at time Wed 11 Dec 2024, 15:04:18.372188
(1733929458.3721879) uuid be0e1646-9579-4b18-8186-9cdb88e6b365
--------------------------------
POST /v1/b HTTP/1.1
user-agent: analytics-flutter/1.0.0
content-type: application/json; charset=utf-8
accept-encoding: gzip
content-length: 24772
host: api.segment.io

"batch": [{"_metadata": {
…
"event": "enter_name",
"integrations": {},
"messageId": "05a984aa-9a75-4e48-9043-bac44c0cd42c",
"properties": {
"ApInstanceId": "1494FB8F94B04CC28534857CDA4CF536",
"name": "Penelope ",
"screen_name": "profile_setup_name"
},
"timestamp": "2024-12-11T10:04:32.390533",
"type": "track",
"userId": "YYS0LcqBKg"
…
"event": "enter_birthdate",
"integrations": {},
"messageId": "ce038bbd-75b8-4fe3-886e-ae474ab05828",
"properties": {
"ApInstanceId": "1494FB8F94B04CC28534857CDA4CF536",
"birthday": "1991-2-8",
"screen_name": "profile_setup_birthday"
},
"timestamp": "2024-12-11T10:04:46.223223",
"type": "track",
"userId": "YYS0LcqBKg"
…
```


41. As shown by the blue highlights in the above excerpt of the App's transmissions, Segment intercepts the name and birthday of the App user (here, "Penelope"; "1991-2-8"). As shown by the red highlights, Segment intercepts the Just A Baby account user ID (here, "YYS0LcqBKg").

//

42. As shown by the green highlights in the above excerpt of the App's transmissions, Segment intercepts the relationship status of the App user (here, "Single"), and the beginning and end of the timeline in which the user "want[s] to make babies" (here, "2025"; "2026"). As shown by the red highlights, Segment intercepts the Just A Baby account user ID (here, "YYS0LcqBKg").

//

//

//

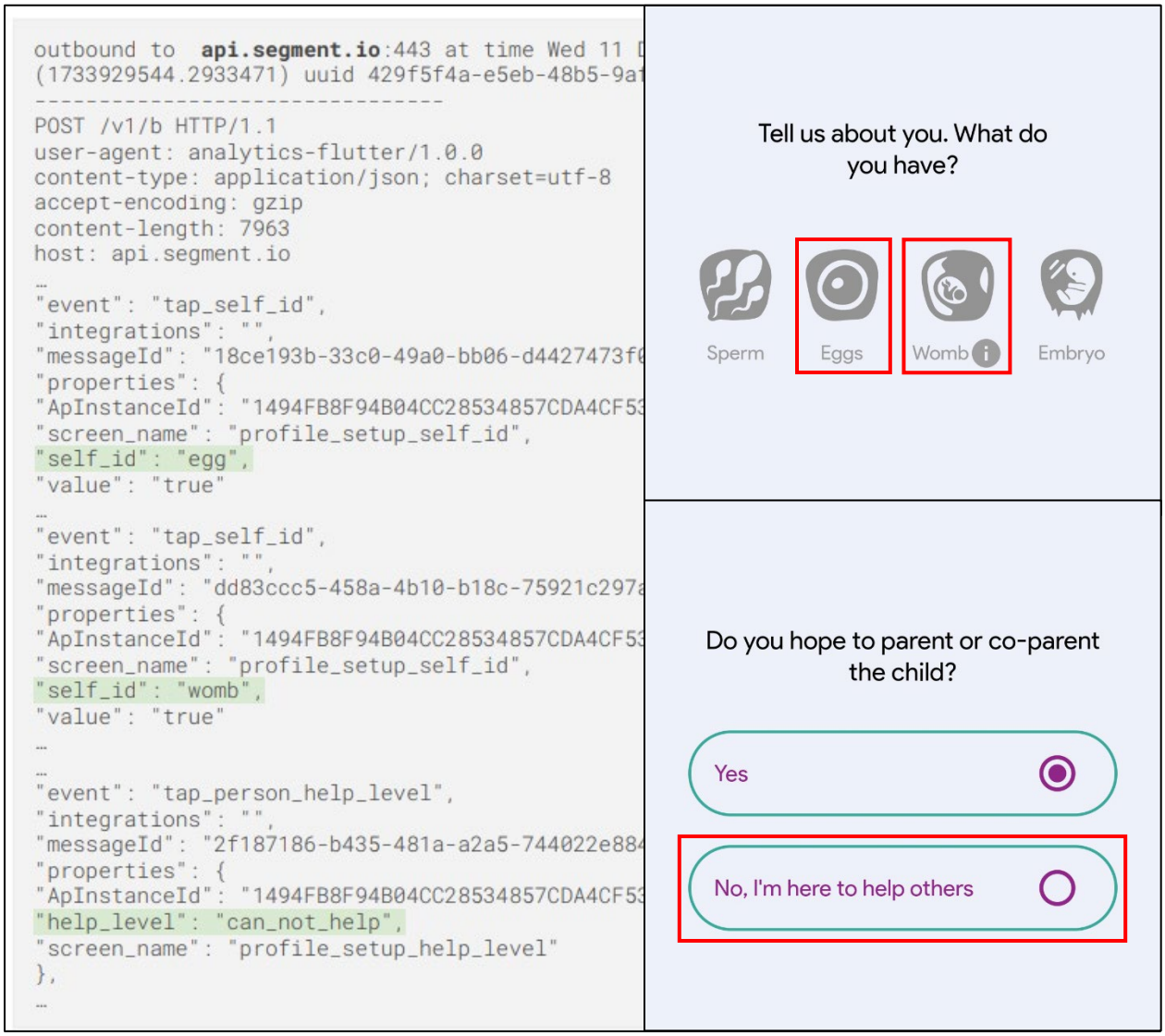
//

//

//

//

//



43. As shown by the green highlights in the above excerpt of the App's transmissions, Segment intercepts when App users provide their fertility information (here, the user has "egg[s]" and a "womb") and whether the user "hope[s] to parent or co-parent the child" (here, the user "can_not_help" with parenting or co-parenting the child).

//

//

//

44. As shown by the green highlight in the above excerpt of the App's transmissions, Segment intercepts when App users provide their written profile description (here, "I[]m finally ready to try this"; meaning, a user is finally ready to try to conceive a child through alternative conception methods). App users provide descriptions because "[q]uality descriptions get more matches[.]"

VI. SEGMENT USES CLASS MEMBERS' DATA FOR ITS OWN PURPOSES

45. When Segment uses its wiretaps on Website users' communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. Instead, Segment—a separate and distinct entity from the parties to the conversations—use the wiretaps to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. Segment itself collects the contents of said conversations.

46. Segment has the capability to use the contents of conversations it collects through its wiretap for its own purposes.

47. In the "Twilio Terms of Service," Segment states that "[Defendant] grants Twilio

and its Affiliates the right to process Customer Data as necessary to provide the Services in a manner that is consistent with this Agreement and the Twilio Data Protection Addendum."[18]

48. "Customer Data" means "any data (a) provided by you or your End Users (as defined below) to Twilio in connection with your use of the Services or (b) generated for your use as part of the Services."[19] "Twilio Data Protection Addendum" means "the personal data processing-related terms for the Services …."[20]

49. Twilio's Data Protection Addendum admits that Segment "processes" "Customer Account Data" to, *inter alia*, "develop and improve new products and services and improve the performance, functionality, safety, and security of the Services[,]"[21] including the Segment Services.

50. Thus, Segment has the capability to use the wiretapped data for purposes other than simply providing a recording to Defendant, including but not limited to operating and improving Segment's own services and products.

CLASS ALLEGATIONS

51. **Class Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and other similarly situated individuals defined as all persons who used the App in California and had their personally identifiable information or protected health information disclosed to Segment (the "Class").

52. Plaintiff reserves the right to modify the Class definition, including by using

[18] TWILIO, TWILIO TERMS OF SERVICE, https://www.twilio.com/en-us/legal/tos.

[19] *Id.*

[20] *Id.*

[21] TWILIO, TWILIO DATA PROTECTION ADDENDUM, https://www.twilio.com/en-us/legal/data-protection-addendum.

subclasses, as appropriate based on further investigation and discovery obtained in the case.

53. The following people are excluded from the Class: (1) any Judge presiding over this action and members of her or her family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

54. **Numerosity:** The number of persons within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class render joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

55. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary between members of the Class, and which may be determined without reference to the individual circumstances of any Class member, include, but are not limited to, the following: whether Defendant violated CIPA §§ 631 and 632 and CMIA § 56.10 and whether Plaintiff and the proposed Class members are entitled to damages, reasonable attorneys' fees, prejudgment

interest and costs of this suit.

56. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, created a Just a Baby account, logged into her account on her Apple iOS device, and, as a result of Defendant's unlawful conduct, had her confidential electronic communications, personally identifiable information, and PHI intercepted and disclosed to a Third Party.

57. **Adequate Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and her counsel.

58. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Classes. Each individual member of the Class may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631(a)

59. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

60. Plaintiff brings this Count individually and on behalf of the members of the Class.

61. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

62. CIPA § 631(a) is not limited to phone lines, but also applies to "new technologies"

such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

63. Segment's tracking technology is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

64. Segment is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, Segment has the capability to use the wiretapped information for its own purposes. Accordingly, Segment was a third party to any communication between Plaintiff and Class Members, on the one hand, and Defendant, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

65. At all relevant times, by their tracking technologies, Segment willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and Class Members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

66. At all relevant times, Segment used or attempted to use the communications intercepted by its tracking technologies for its own purposes.

67. At all relevant times, Defendant aided, agreed with, employed, permitted, or otherwise enabled Segment to wiretap Plaintiff and Class Members using Segment's tracking technologies and to accomplish the wrongful conduct at issue here.

68. Plaintiff and Class Members did not provide their prior consent to Segment's intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff's and Class Members' electronic communications. Nor did Plaintiff and Class Members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling Segment's conduct.

69. The wiretapping of Plaintiff and Class Members occurred in California, where Plaintiff and Class Members accessed the Website and where Segment – as enabled by Defendant – routed Plaintiff's and Class Members' electronic communications to Segment's servers.

70. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT II
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 632

71. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

72. Plaintiff brings this claim against Defendant individually and on behalf of the members of the Class.

73. CIPA § 632(a) prohibits an entity from:

> intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

74. The Third Parties' tracking technologies are "electronic amplifying or recording device[s]." *Id.*

75. Cal. Civ. Code § 56.05(j) states:

> "Medical information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care … regarding a patient's … reproductive or sexual health application information, mental or physical condition, or treatment.

76. Per Cal. Civil Code § 56.10(a):

> A provider of health care … shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c).

77. Here, App users' communications with Defendant—made while affirmatively interacting with the App—contain protected "medical information," as defined by Cal. Civil Code § 56.05.

78. First, the communications include "individually identifiable information[.]" Cal. Civil Code § 56.05. Defendant enables Segment to identify individual App users with the Segment API, which collects names, phone numbers, dates of birth, App user IDs, and users' IP addresses which, "alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code § 56.05(j).

79. Second, App users' communications with Defendant "regard[] a patient's … reproductive or sexual health application information, mental or physical condition, or treatment." *Id.* Segment intercepts App users' private communications such as fertility information, relationship status, and written profile description, all of which pertain to users' efforts to conceive a child through alternative conception methods.

80. Thus, Segment—as aided by Defendant—intercepted "medical information," which is protected, under Cal. Civil Code § 56.10.

81. When communicating with Defendant, Plaintiff and Class Members had an objectively reasonable expectation of privacy, based on Cal. Civil Code § 56.10. Thus, Plaintiff

and Class Members did not reasonably expect that anyone other than Defendant would be on the other end of the communication, and that other third-party entity Segment would intentionally use an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

82. Plaintiff and Class Members did not consent to any of Segment's actions. Nor have Plaintiff or Class Members consented to Segment's intentional use of an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

83. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 632(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 632(a).

COUNT III
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56.10

84. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

85. Plaintiff brings this Count individually and on behalf of the members of the Class.

86. Under the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10 ("CMIA"), providers of health care are prohibited from disclosing medical information relating to their patients, without a patient's authorization.

87. Medical information means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's … reproductive or sexual health application information, mental or physical condition, or treatment." CMIA § 56.05(j). "'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow

identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." *Id*.

88. CMIA § 56.06(a) defines a provider of health care as "[a]ny business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information, or for the diagnosis and treatment of the individual[] …." CMIA § 56.06(f) says that "[a]ny business described in this section shall maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to the business."

89. CMIA § 56.06(e) provides that "[a]ny business that offers a reproductive or sexual health digital service to a consumer for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part."

90. CMIA § 56.05(r) provides that a "'[r]eproductive or sexual health digital service' means a mobile-based application or internet website that collects reproductive or sexual health application information from a consumer, markets itself as facilitating reproductive or sexual health services to a consumer, and uses the information to facilitate reproductive or sexual health services to a consumer."

91. Per CMIA § 56.05(q), "'[r]eproductive or sexual health application information' means information about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive, or type of sexual activity collected by a reproductive or

sexual health digital service, including, but not limited to, information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity."

92. Plaintiff and Class Members are patients under the definition of the CMIA because Plaintiff and Class Members "received health care services from a provider of health care" and the information Defendant shared to Segment was "medical information pertain[ing]" to Plaintiff and Class Members. CMIA § 56.05(m).

93. Defendant is a provider of health care under CMIA § 56.06 because it is a "business that offers a reproductive or sexual health digital service to a consumer for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual …." CMIA § 56.06(e). Because Defendant is deemed a provider of health care, it has an ongoing obligation to comply with the CMIA's requirements regarding the maintenance of its user's medical information.

94. As set forth hereinabove, names, phone numbers, dates of birth are sufficient to allow identification of an individual. Along with patients' names, phone numbers, and dates of birth, Defendant disclosed to Segment several pieces of information regarding its patients' use of its App, which, on information and belief, includes but was not limited to: patients' communications relating to their relationship status, patients' fertility information, and patients' written profile descriptions, all of which pertain to pertain to users' efforts to conceive a child through alternative conception methods.

95. This patient information is derived from a provider of health care regarding patients' medical treatment and physical condition. Accordingly, it constitutes medical information pursuant to the CMIA.

96. Defendant, as set forth hereinabove, failed to obtain its patients' valid authorization for the disclosure of medical information to Segment, which is done for marketing, advertising, and analytics purposes.

97. Pursuant to CMIA § 56.11, a valid authorization for disclosure of medical information must: (1) be "[c]learly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization"; (2) be signed and dated by the patient or her representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires.

98. Based on the above, Defendant violated the CMIA by disclosing its patients' medical information to Segment, along with the patients' names, phone numbers, and dates of birth.

99. Under the CMIA, a patient may recover compensatory damages, punitive damages not to exceed $3,000 dollars and attorneys' fees not to exceed $1,000, and the costs of litigation for any violating disclosure of medical information. Alternatively, a patient may recover nominal damages of $1,000 for any negligent release of medical information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendants' conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For actual, compensatory, statutory, and/or punitive in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses, as well as costs of suit.

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: March 10, 2025

Respectfully submitted,

By: */s/ Yitzchak Kopel*
Yitzchak Kopel

BURSOR & FISHER, P.A.
Yitzchak Kopel
Max S. Roberts
Victoria X. Zhou
1330 Avenue of the America, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: ykopel@bursor.com
mroberts@bursor.com
vzhou@bursor.com

Attorneys for Plaintiffs